4 security warnings you should not 'ignore'

When you are performing activities on the Internet and suddenly a warning is issued from your web browser or operating system, you should take care of it and it is important to act in a timely manner.

When you are performing activities on the Internet and suddenly a warning is issued from your web browser or operating system, you should take care of it and it is important to act in a timely manner.

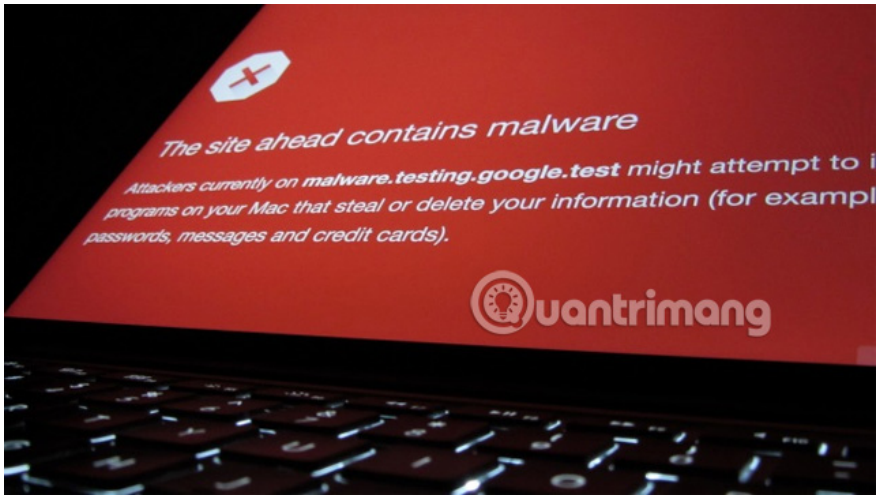
Examples of such warnings:

1. 'The site ahead contains malware' (The website is intended to contain malware)
2. 'Có m?t v?n ?? v?i ch?ng nh?n Security website này' (The security certificate of this site has a problem)
3. 'Windows Firewall ?ã có l? m?t s? c?a ph?n này' (Windows Firewwall has blocked some features of this app)
4. 'Turn on virus protection' (Enable antivirus protection)

These alerts sometimes appear when browsing the web, playing online games or installing Internet-based software. But what do you do when you see these warnings? And what do these Internet security warnings mean?

It's time to find out why you shouldn't ignore these four security warnings and what to do to deal with them. The article will explain these four warnings and what to do when you see them.

1. Warning "The Site Ahead Contains Malware"



Have you ever done a web browser, clicked on a link and found this warning ' **The Site Ahead Contains Malware** '? Thanks to Chrome's secure browsing tool (a feature built into popular browsers), you'll see the message: the site you're about to visit could be infected with malware (the site you're about to visit) Access may be infected with malware) if the site is not secure. Therefore, instead of continuing to access, you should close the browser tab and search for a safer website.

1. How to protect and browse safely with Google Chrome?

If you use other browsers such as Internet Explorer and Edge, you will see a warning 'This website has been reported as unsafe' (This site is reported to be unsafe) or on Mozilla Firefox as a warning 'Deceptive site ahead '(The website you are trying to access may be a phishing site) or a' Reported attack page 'warning (The site is reportedly attacked) on older Mozilla Firefox versions.

Warnings like this are intended to prevent users from accessing websites that distribute malware, it could be a virus, Trojan or ransomware. Keeping online safe means avoiding phishing sites, so when you see warnings like "The site ahead contains harmful programs '(Sites that intend to access contain harmful programs) or' This trang th? th? t?i t?p tin t? unauthenticated source. ' (This site is loading scripts from an unauthenticated source.) You should not continue to access, go back to search for a safer website.

Therefore, when you encounter such warnings, you should use any option to return to the secure website. Unless you know the website you are trying to access, you should not click on it to continue access.

2. Warning "There is a Problem With This Security Certificate Website"

If the site's security certificate expires, you will see this warning (especially on Internet Explorer and Edge web browsers) and on Chrome it may be 'The certificate's security server is not yet trusted / yet valid' (The server's security certificate is not trustworthy / invalid).

These problems can occur if the security certificate is not authenticated, usually on sites that use HTTPS rather than sites using HTTP. If you encounter this error, it means that the site has been hacked or it could be a fake website.

Note, if you encounter this warning frequently, check the time on your computer and see if it has been properly synchronized. If not, the security certificate will not be authenticated.

3. Warning "Windows Firewall Has Blocked Some Features of This App"

This is limited to Windows systems but not limited to Windows Firewall. Any firewall software can display a warning like this when a program tries to access it illegally.

1. How does the firewall work?

Normally, a new application will not be on the firewall's built-in whitelist, this is a list of safe applications and games. However, this warning also refers to the activities of malware on computers or hackers trying to steal data.

To learn more about the issue, check the details. This warning will show the name of the software you try to access online, you can distinguish the name of the software publisher by searching the Internet or running antivirus software before allowing the program to run. If safe, you can enable the application through the firewall.

4. Warning "Turn On Virus Protection"

If you've ever seen this warning on Microsoft Windows, this means your antivirus software has been disabled. Sometimes a warning occurs when you have just uninstalled a third-party antivirus software and need to reactivate Windows Defender. However, this may also be a sign of malware infection.

1. Use Windows Defender with Command Prompt on Windows 10

To resolve this issue, re-enable Windows Defender by clicking **Start** and typing **defender** . In the results that appear, click on **Windows Defender Security Center** and search for **Virus & threat protection** . If it comes with a red cross symbol, click **Turn on** . Note Windows Defender Security Center will display third-party security tools.

If the antivirus software cannot reactivate, it may have been blocked, you should immediately scan the system for malware by using a reputable tool like Malwarebytes Antimalware.

Always update your browser and security tools

You now know what to do with these alerts and understand the importance of having a secure browser. If not updated regularly, the browser is easily exploited and this update will protect your computer and data.

It is worth noting that the best online security tools such as a comprehensive security suite with firewall, antivirus, ransomware protection, etc., or specific applications and software, should be used. provide its own protection methods.

Don't ignore the warning, read them

The habit of clicking when browsing is often neglected by safety. Users often ignore alerts and do not read them carefully, but this will make you unprotected and can ignore important messages.

Therefore, it is a habit to read these warnings, consider when they appear and take the time to understand these messages before clicking **OK** . If in doubt, you can search for information on the Internet.

See more:

1. Why do we often ignore browser security warnings?
2. 3 Chrome extensions enhance your security and safety
3. 7 ways to protect your web browser from network attacks

You finished reading the article "**4 security warnings you should not 'ignore'**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.